

1 →

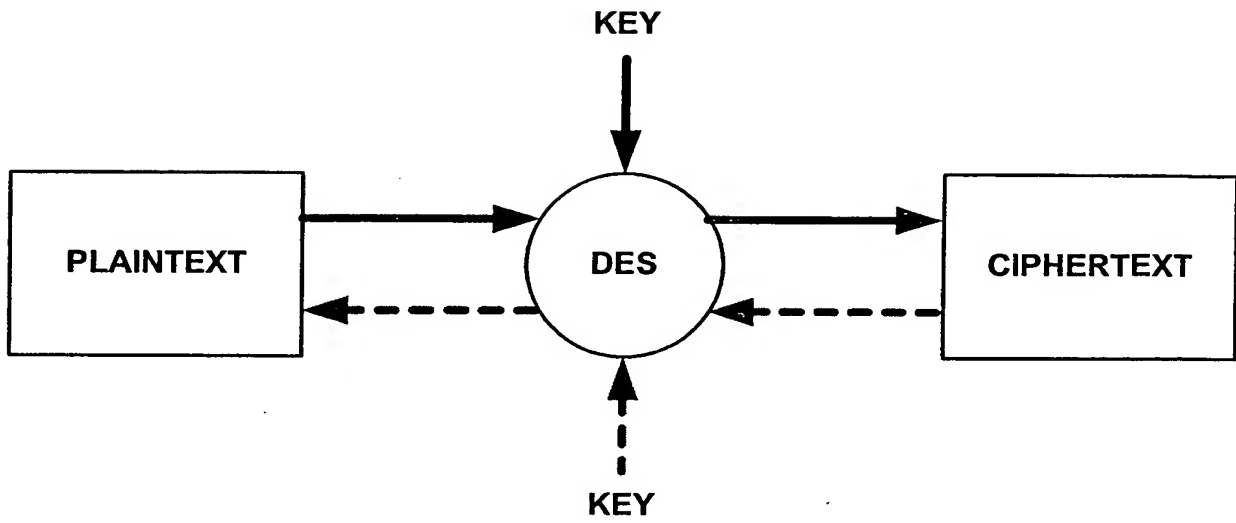
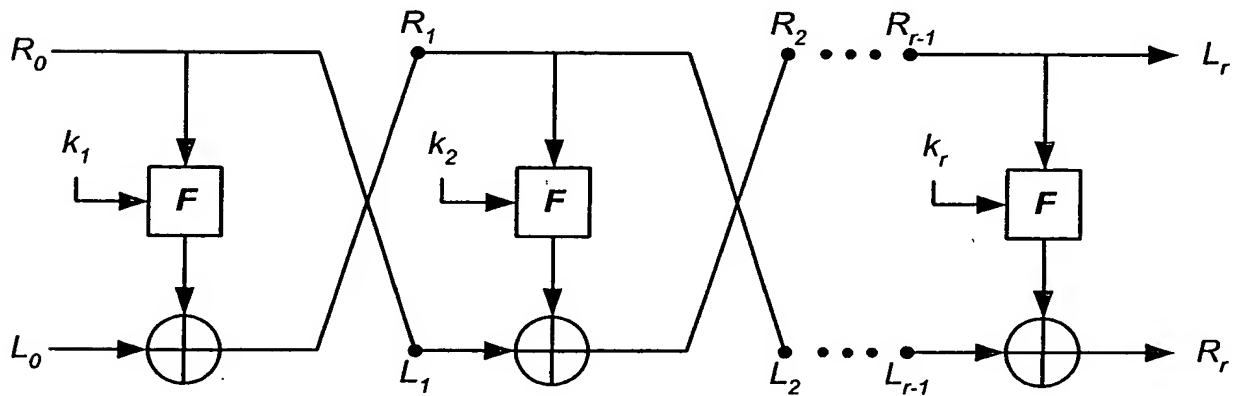


Fig. 1A

2 →



Feistel Cipher

Fig. 1B

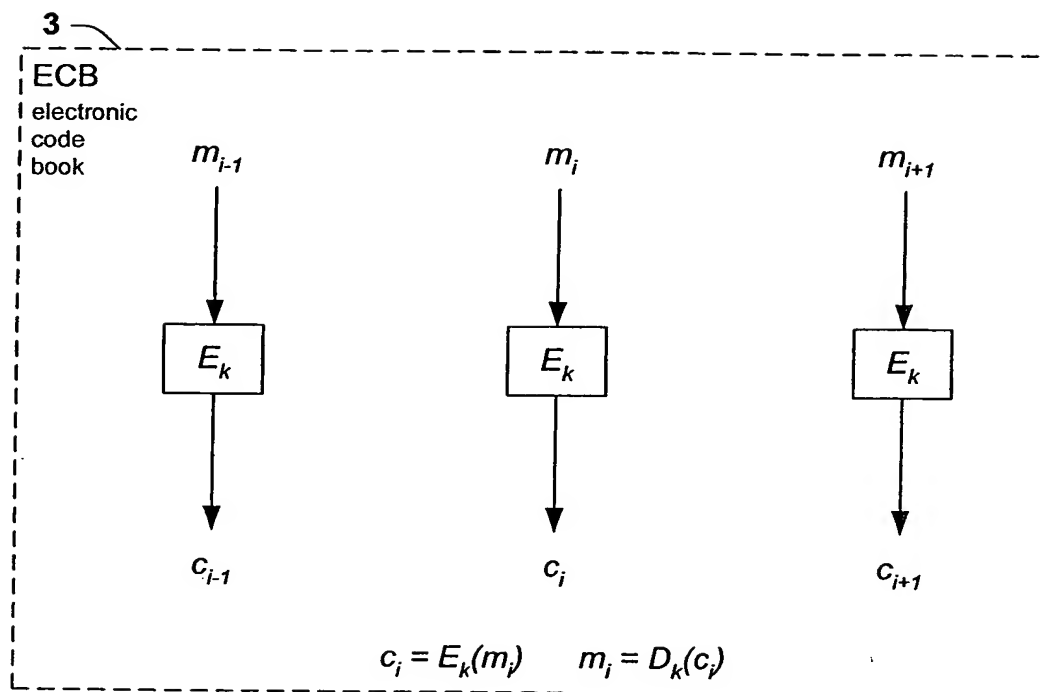


Fig. 1C

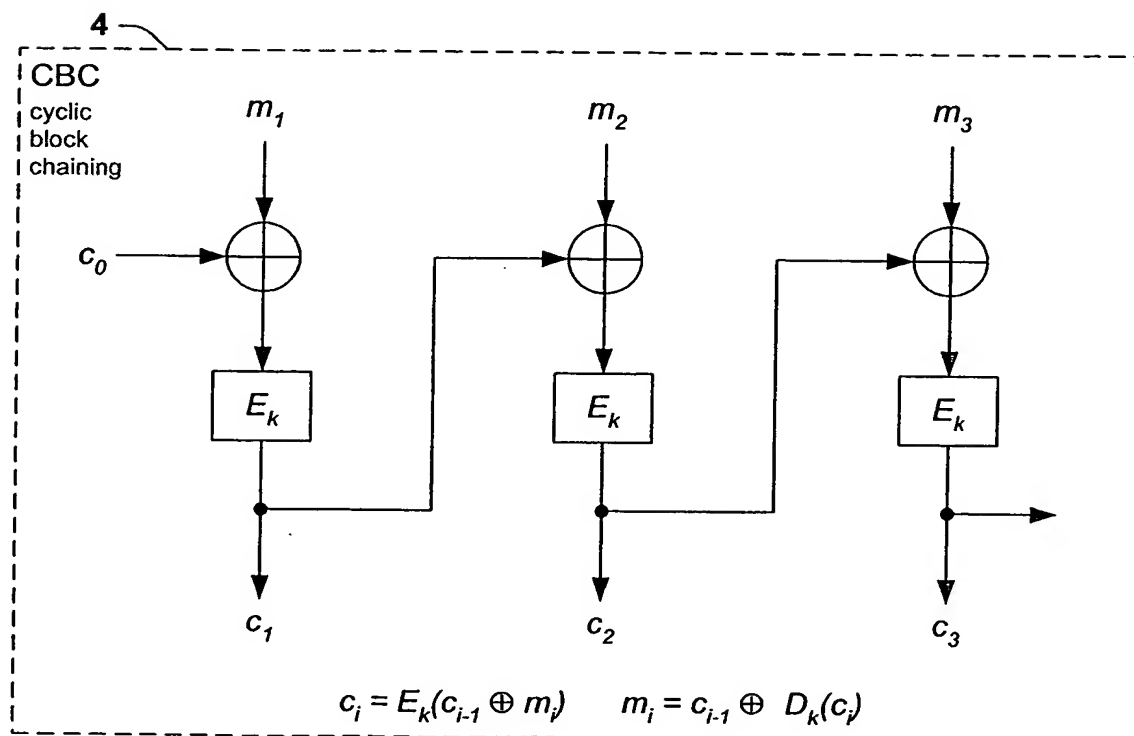


Fig. 1D

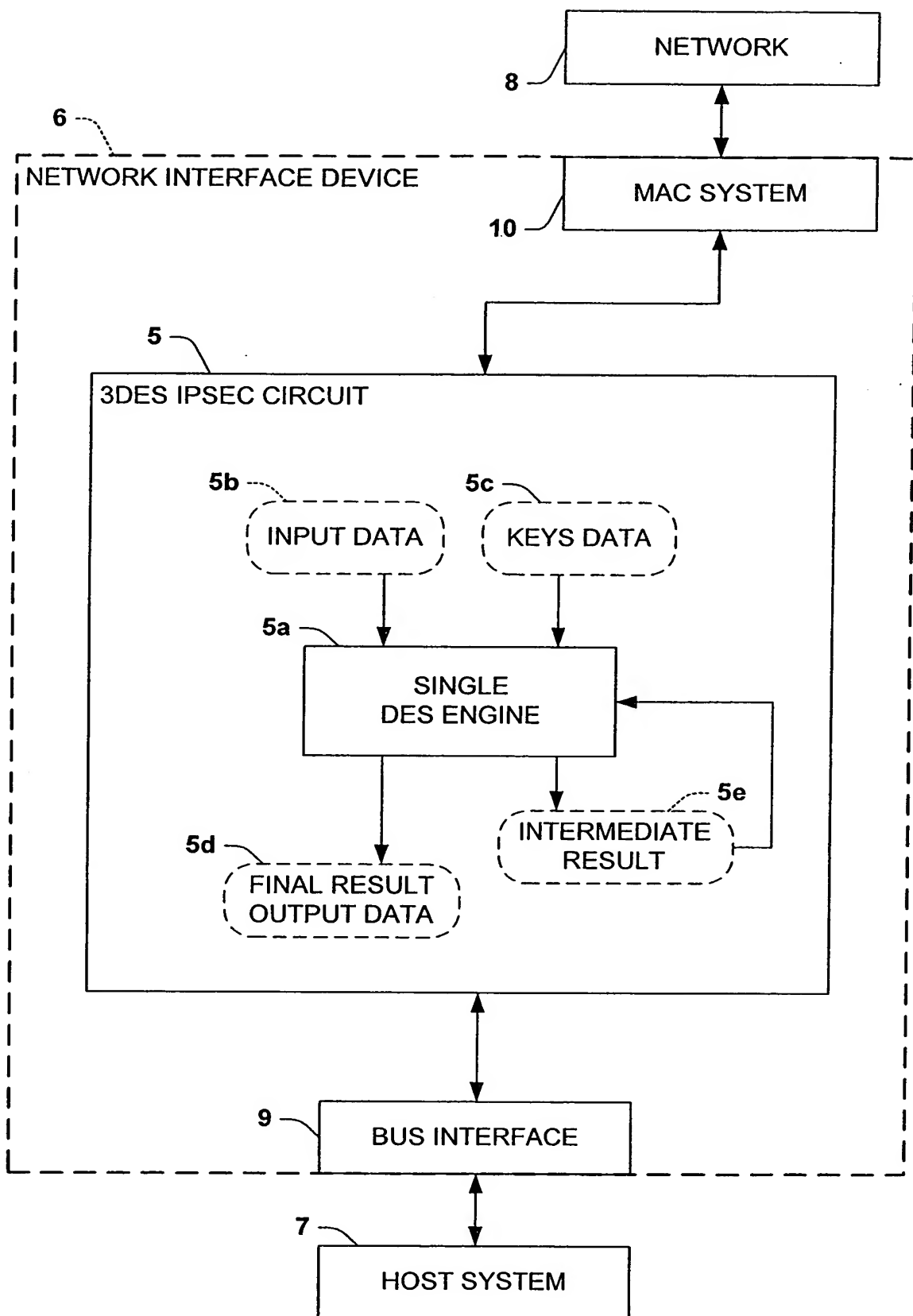


Fig. 1E

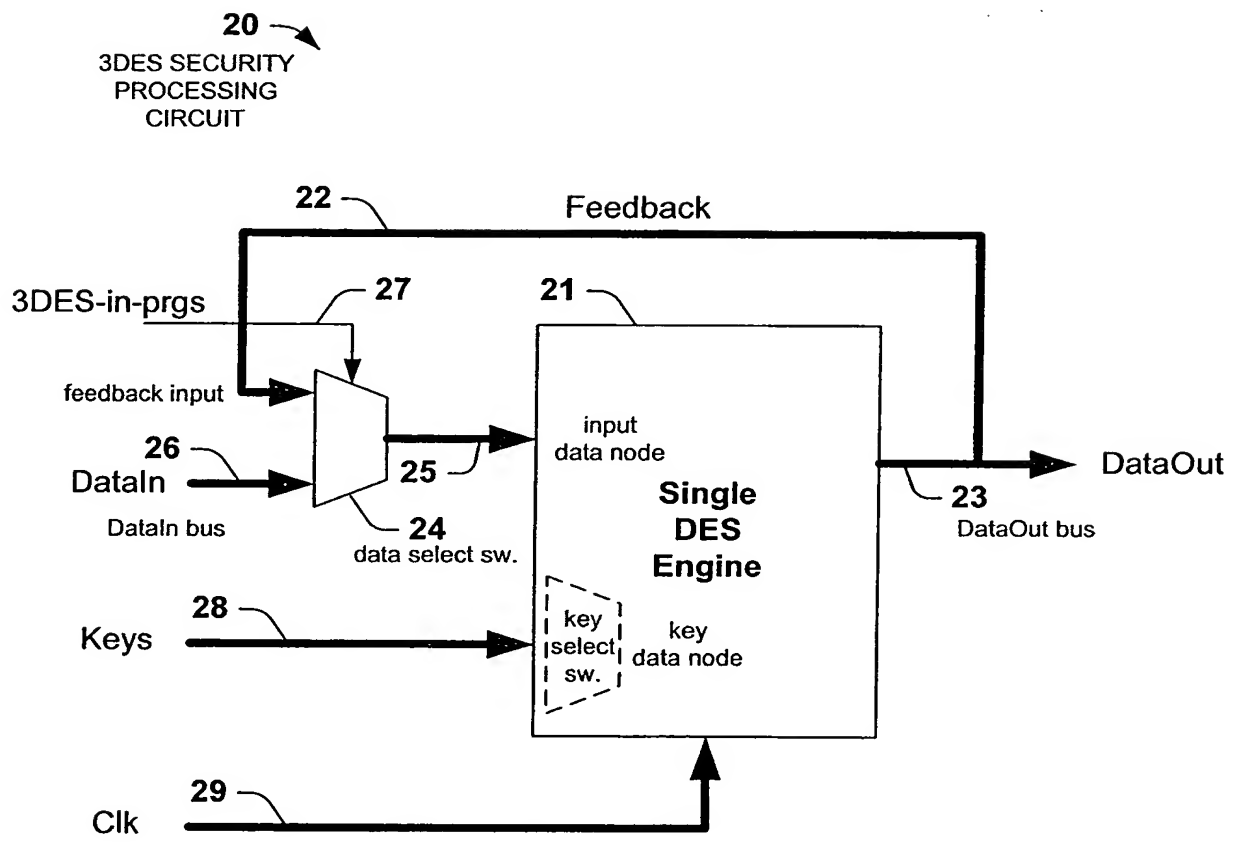


Fig. 1F

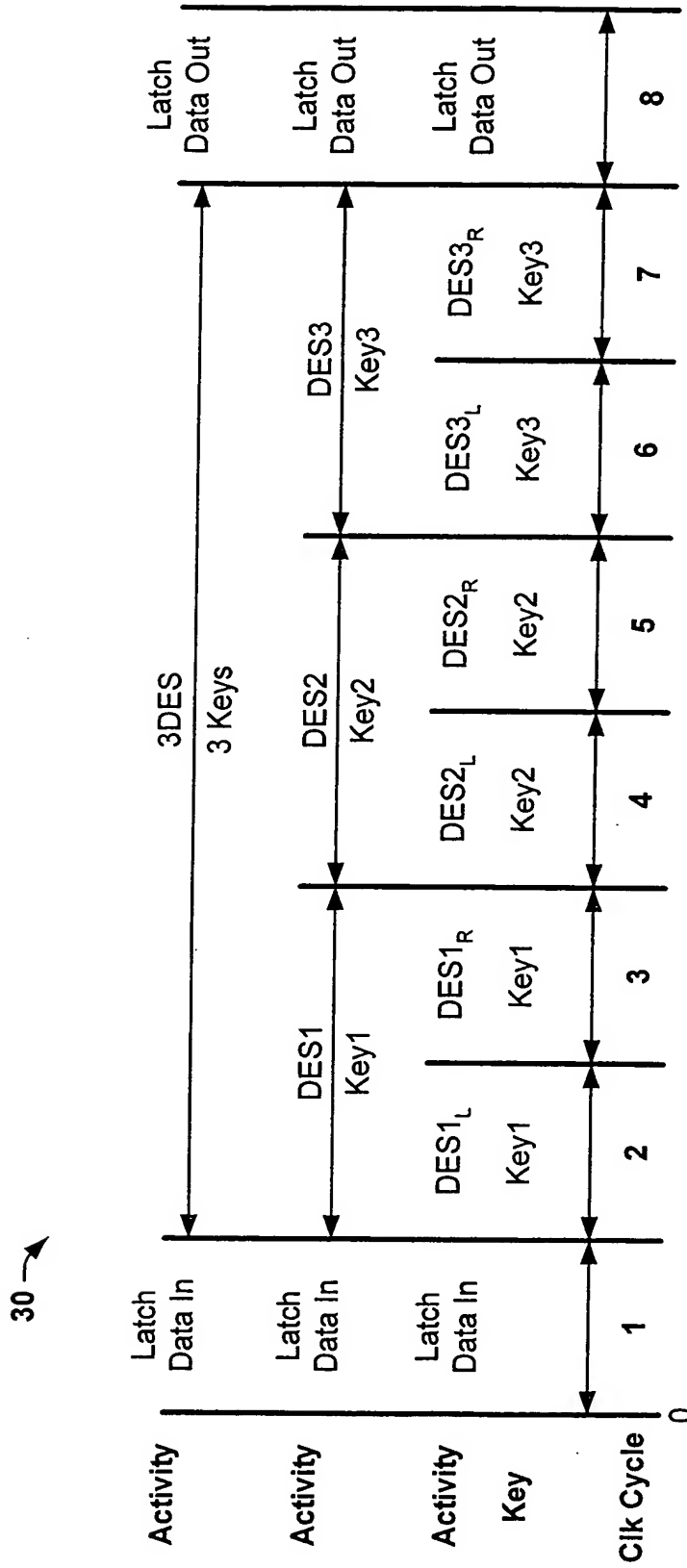


Fig. 1G



6/15

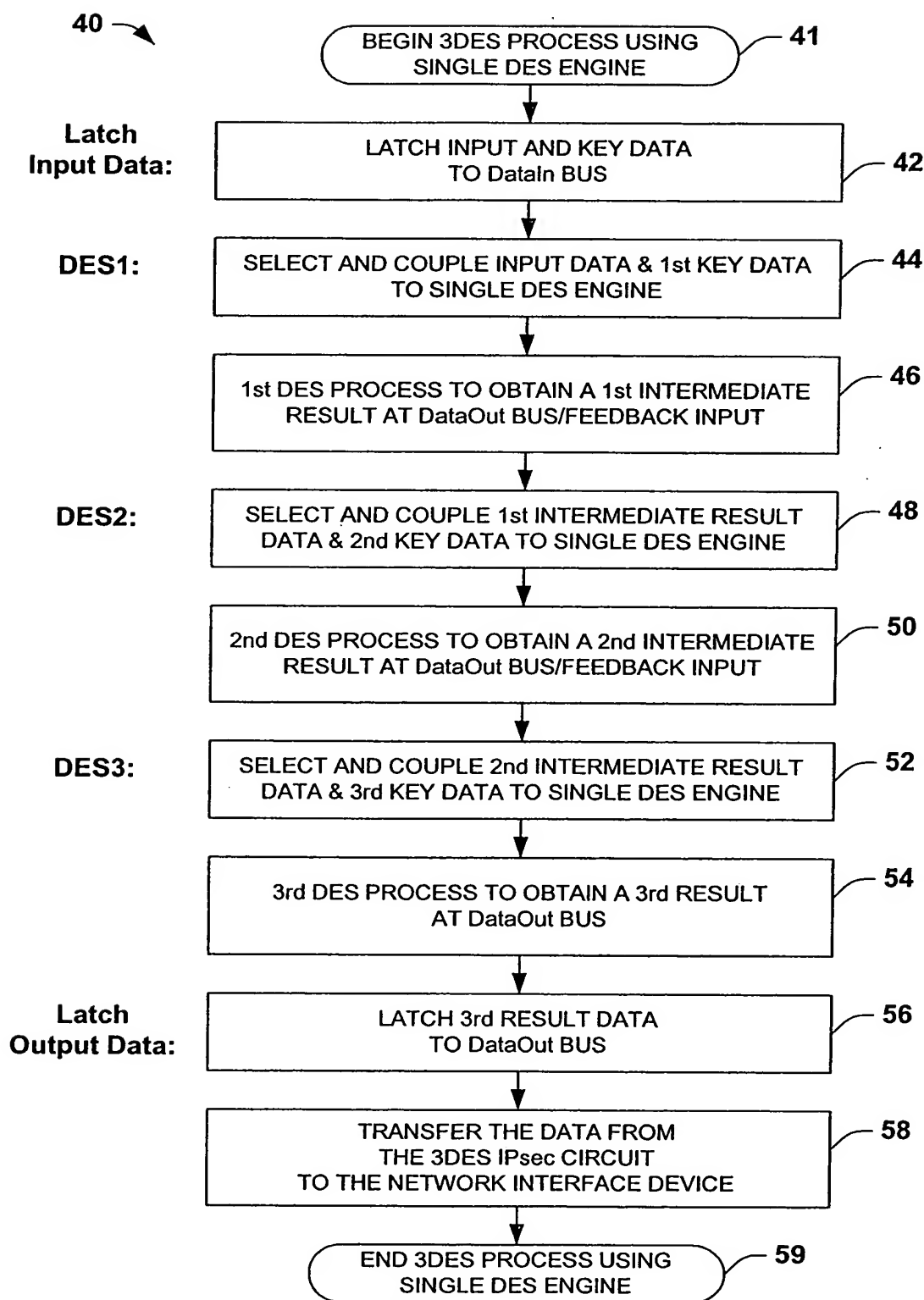


Fig. 1H

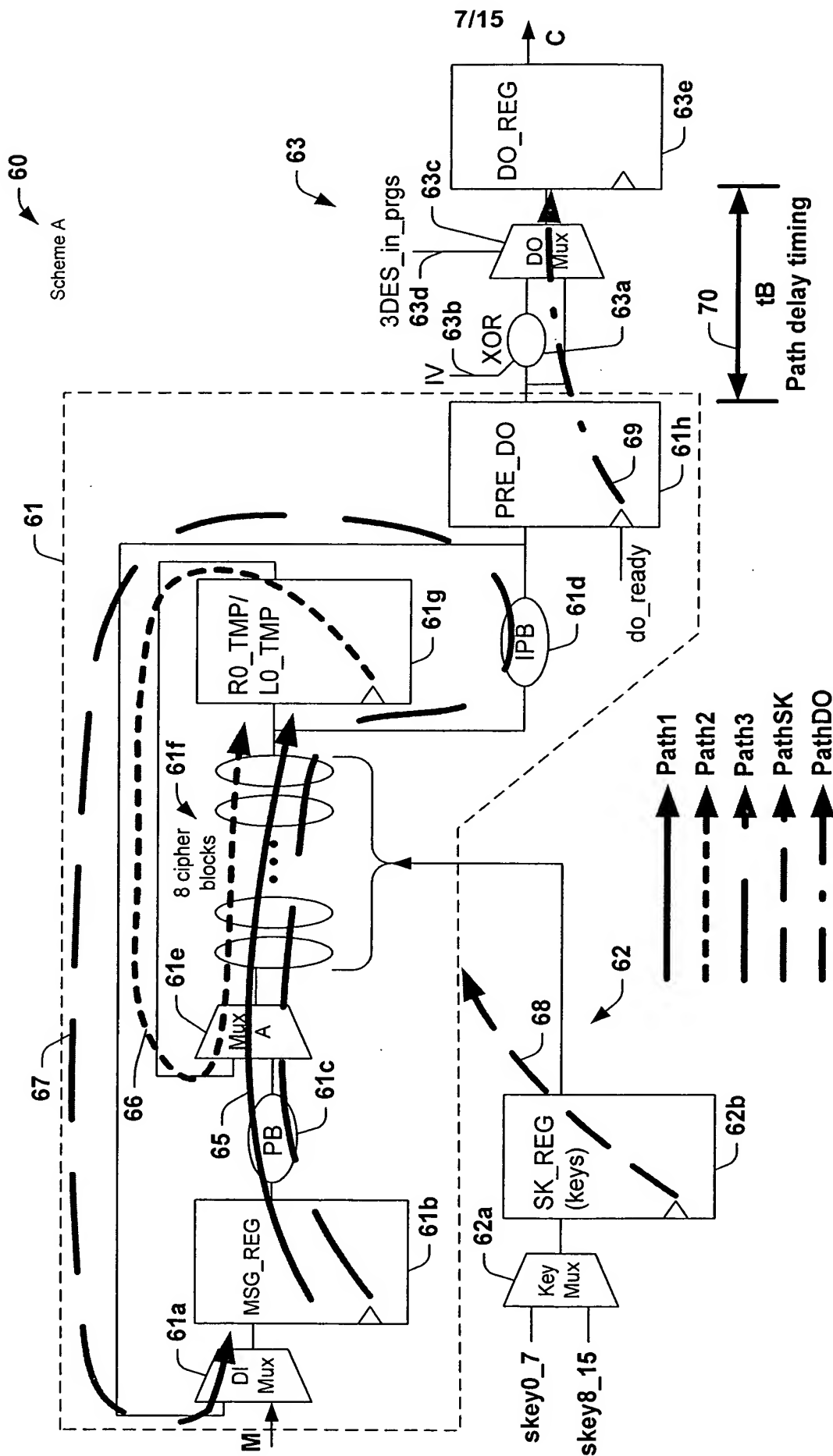
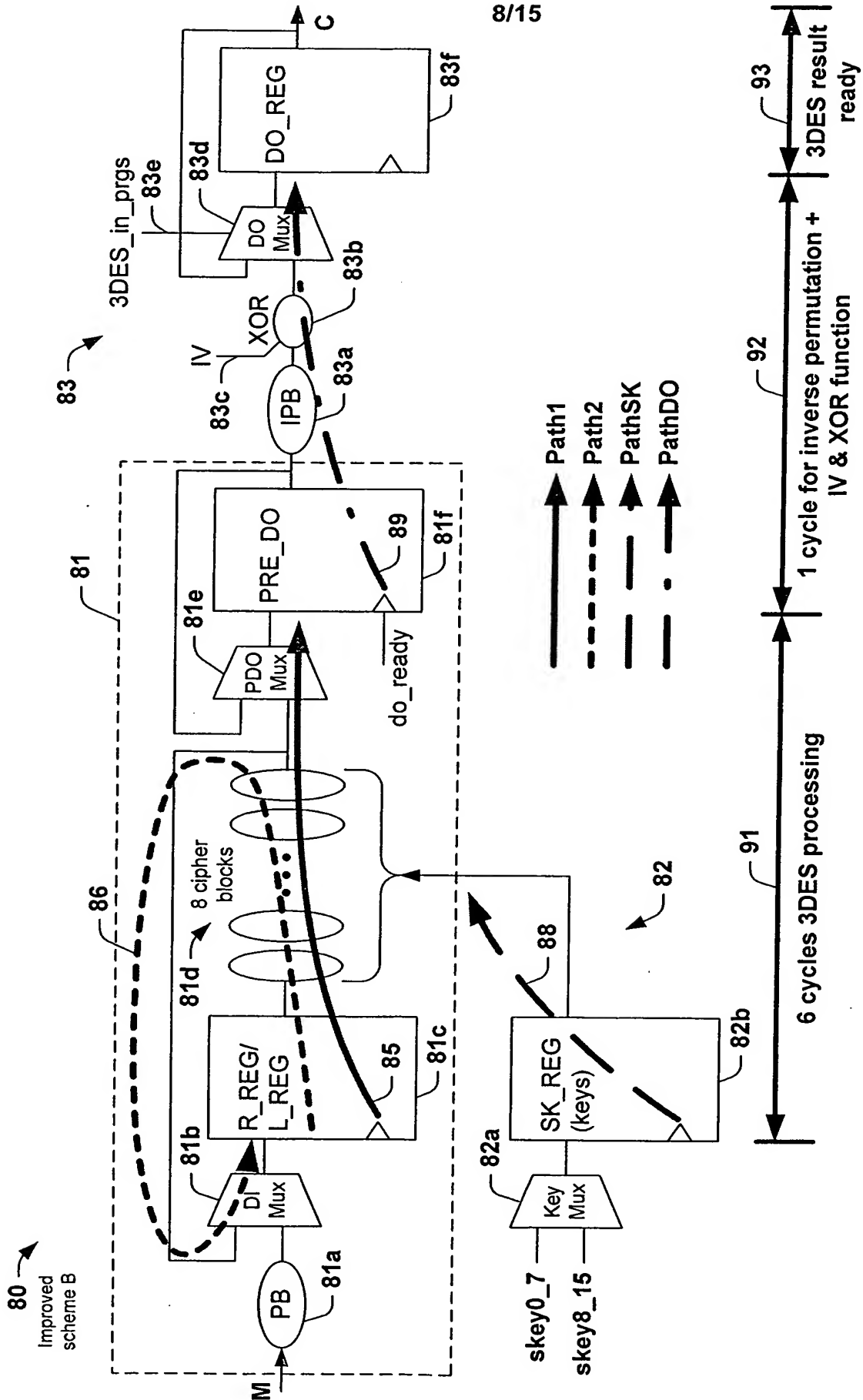


Fig. 11

8/15



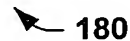




99

Scheme A	Improved Scheme B
Path1 (1st 8 steps)	Path1 (1st 8 steps)
PB	8 Cipher Blks
MuxA	PDO Mux
8 Cipher Blks	
Path2 (2nd 8 steps)	Path2 (2nd 8 steps)
MuxA	8 Cipher Blks
8 Cipher Blks	DI Mux
Path3 (loopback for 3DES)	Path3 (equivalent- 1 or 2)
PB	8 Cipher Blks
MuxA	DI Mux or PDO Mux
8 Cipher Blks	
IPB	
DI Mux	
PathDO	PathDO
IV XOR	IPB
DO Mux	IV XOR
	DO Mux
PathSK	PathSK
8 Cipher Blks	8 Cipher Blks
	PDO Mux

Fig. 1K



**Fig. 2**

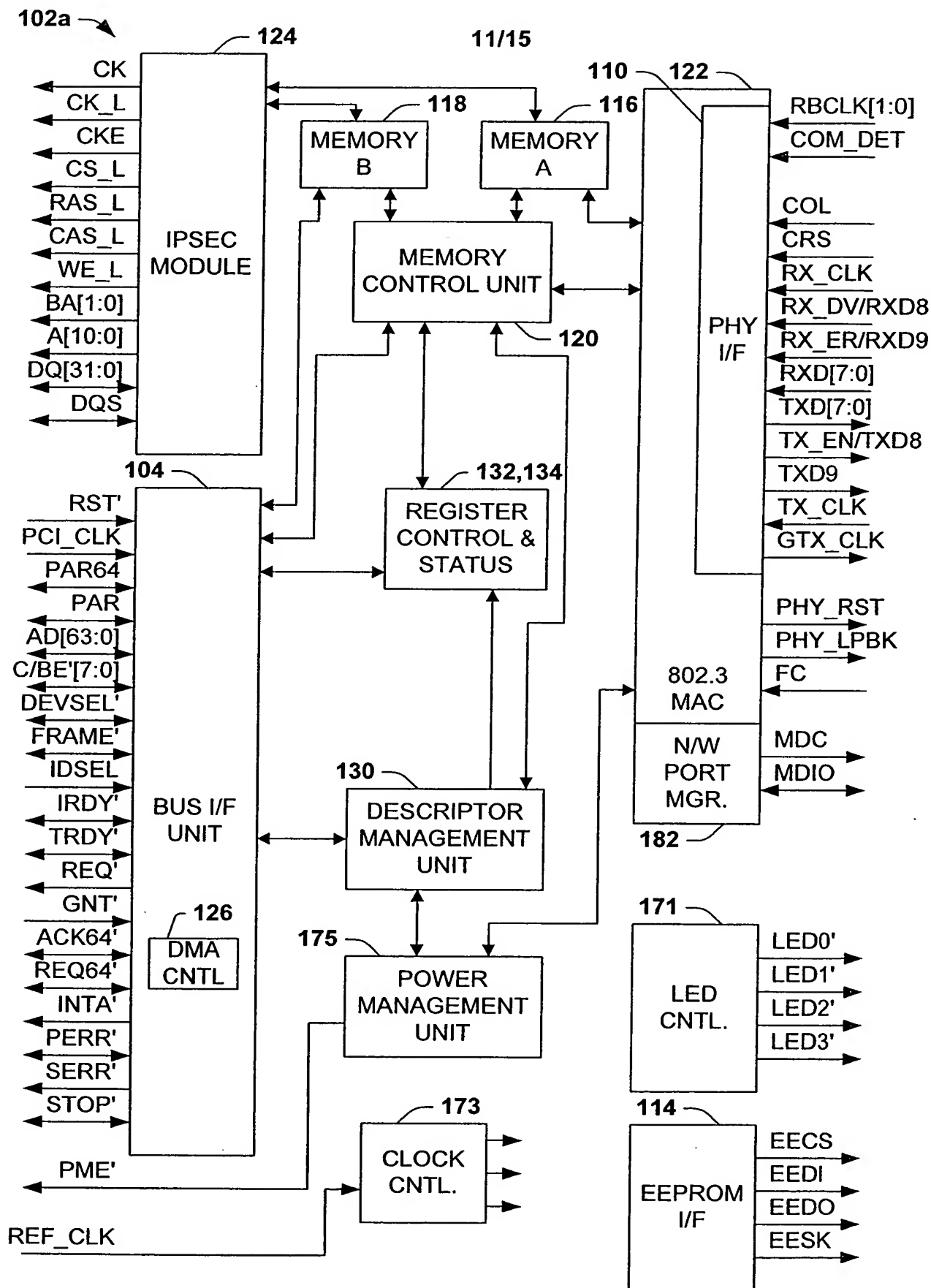


Fig. 3

12/15

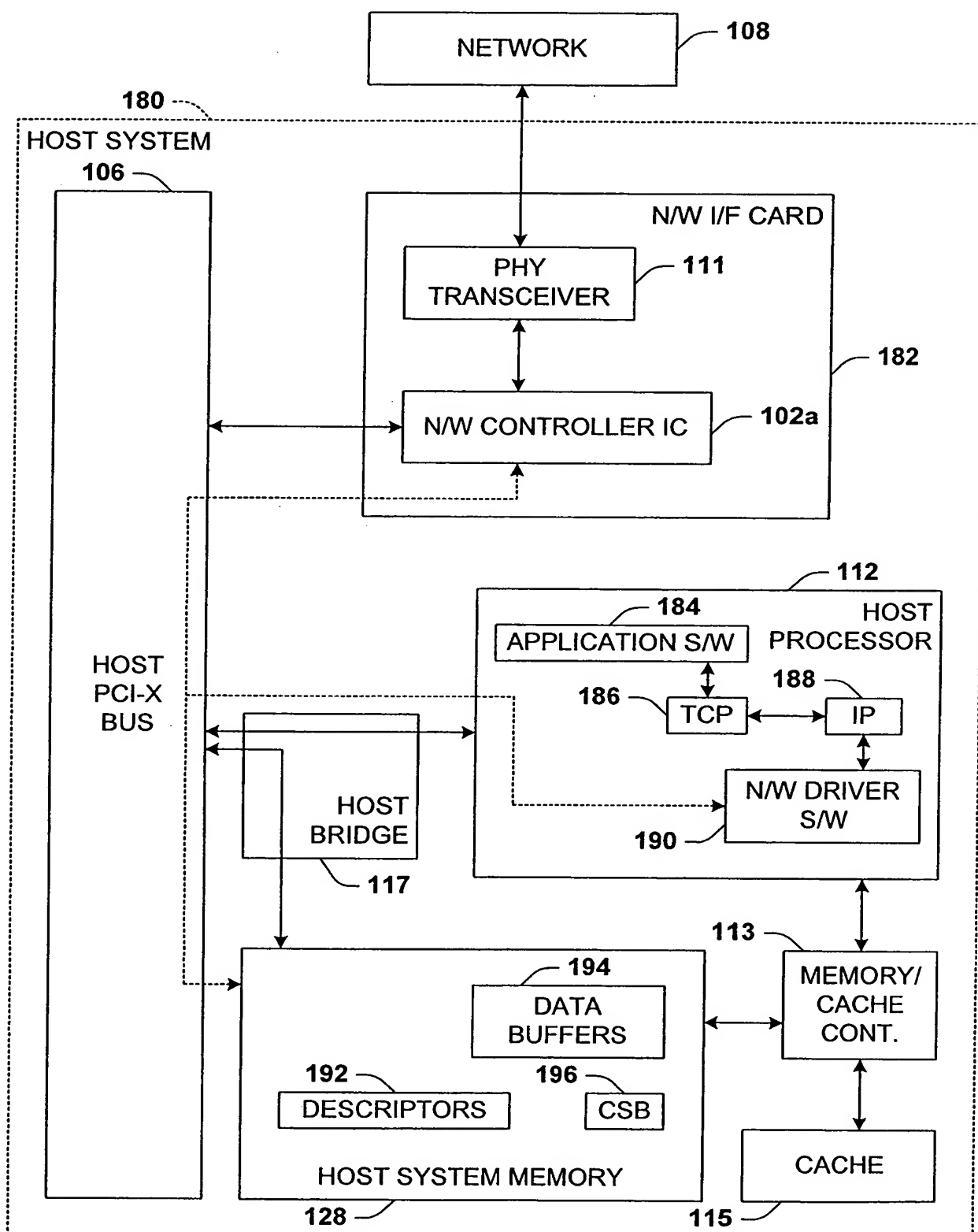
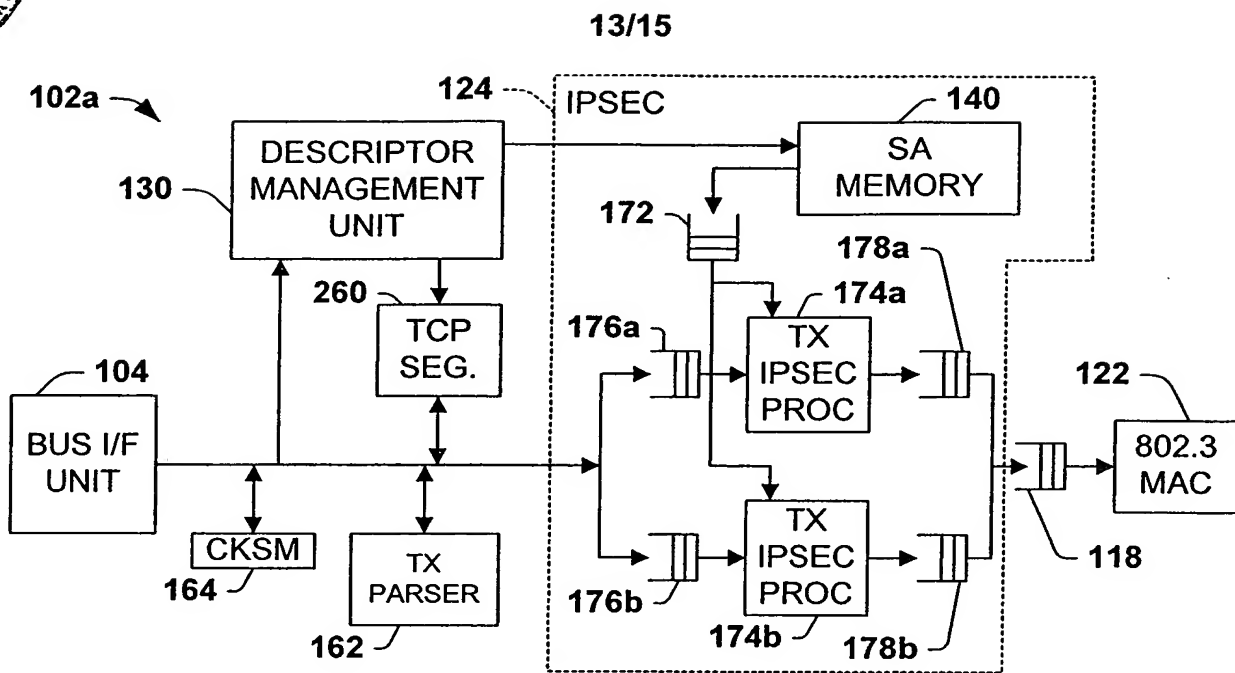
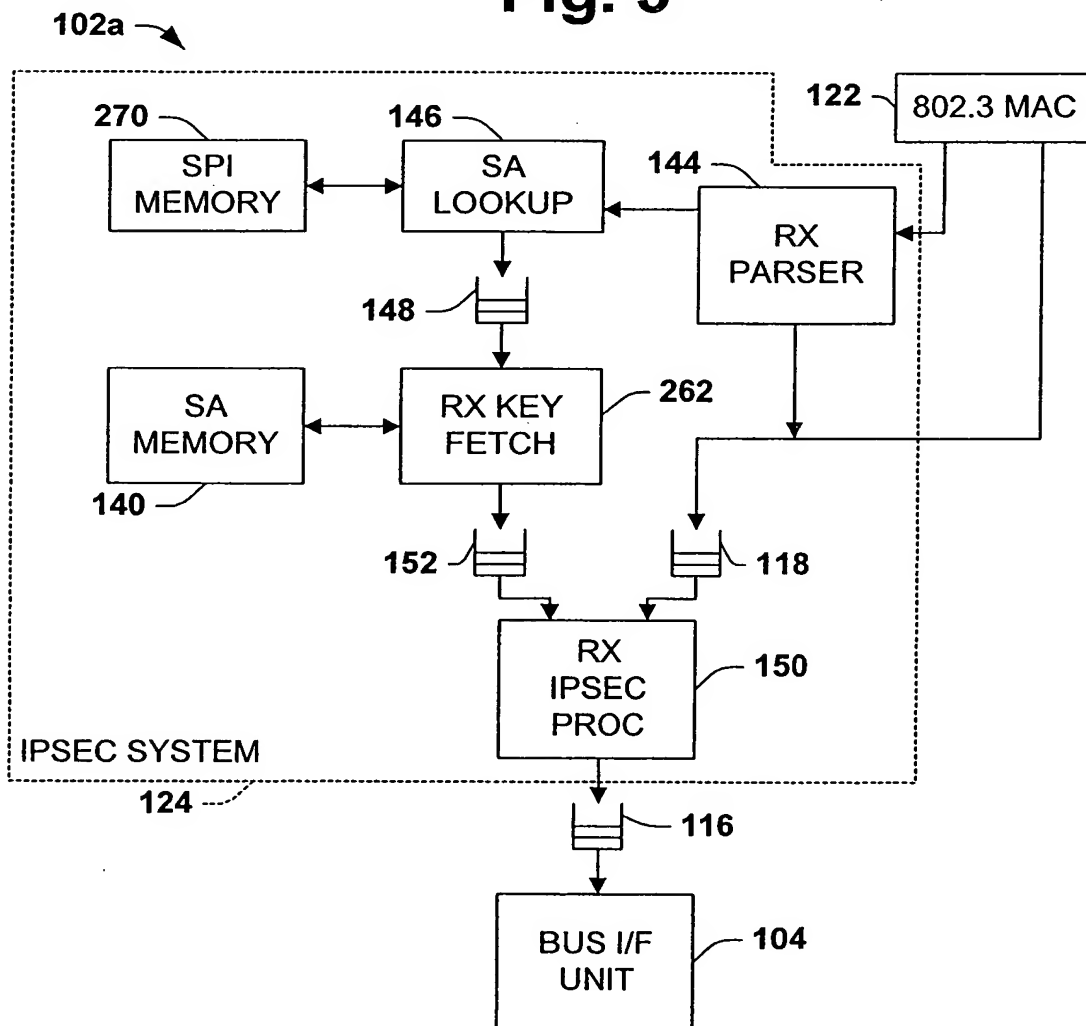


Fig. 4



**Fig. 5**



**Fig. 6**





15/15

140 →

## SA MEMORY ENTRY

274

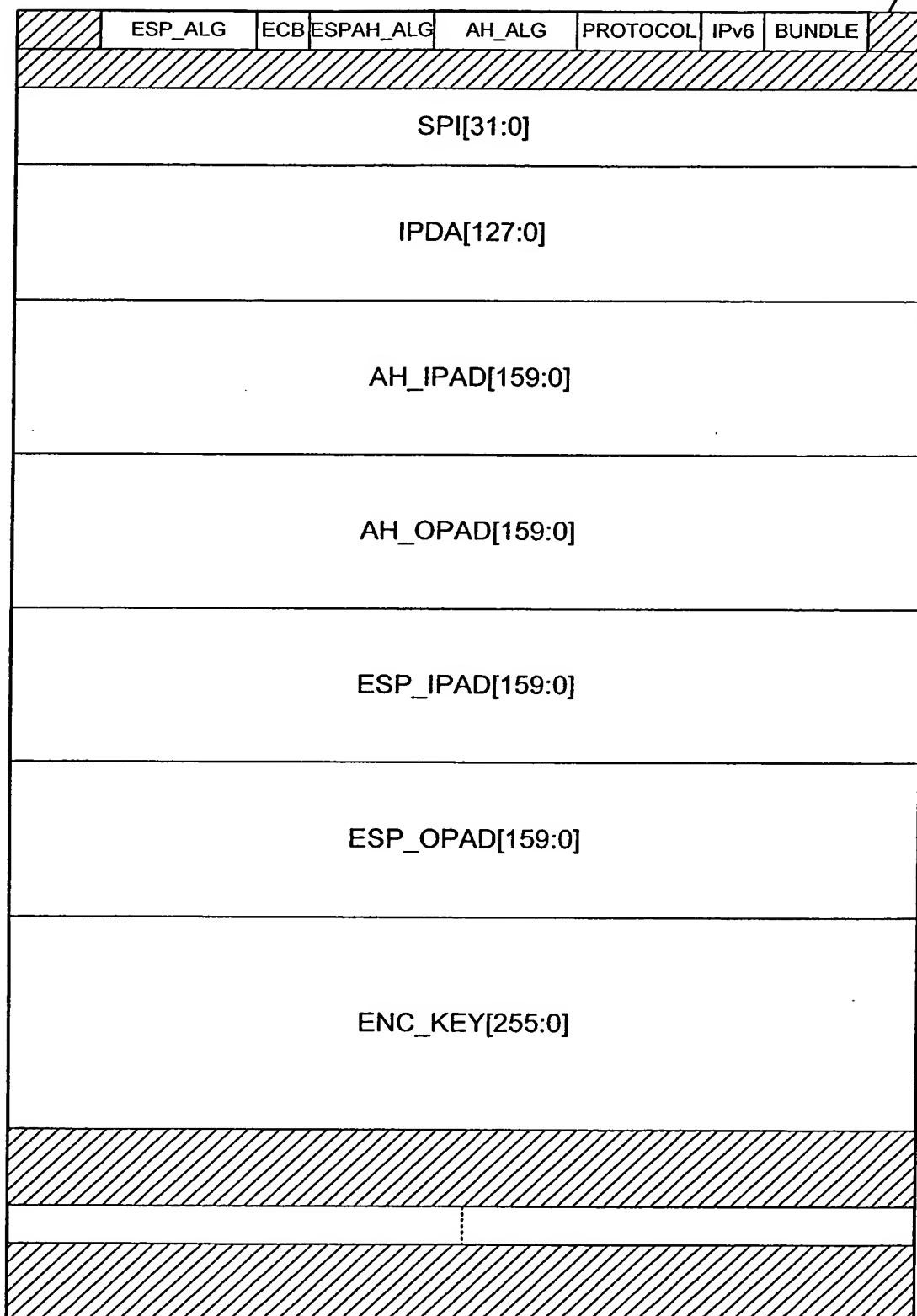


Fig. 7D